Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A digital wallet, secured with a user's access code, for reproducing a confidential datum for said user, said digital wallet comprising:

(a) a computer-implemented input for receiving a input access code;

(b) a seed derivation module operatively connected to said input, for deriving a seed usable to generate at least a portion of said confidential datum;

(c) a seed-based data generation module

(i) implementing a predetermined data generation protocol that was previously used by a seed-based initialization of said confidential datum of said user,

(ii) containing a representation of a seed-access code relationship,

(iii) configured to generate an output datum by digitally processing said derived seed in accordance with said seed-access code relationship, and

(iv) said output datum reproducing said at least a portion of said user's confidential datum if said input access code equals said user's access code; and

(d) said generation of said output datum occurring without dependence on any storage of any form of said at least a portion of said confidential datum~~.~~,

(e) wherein for at least one input access code not equaling said user's access code, said output datum has the characteristic appearance of said at least a portion of said confidential datum, but said output datum does not reproduce at least a portion of said user's confidential datum.

2. (Canceled)

3. (Canceled)

4. (Original) The wallet of claim 1 where said access code is a PIN, and said confidential datum includes an asymmetric cryptographic key.

5. (Original) The wallet of claim 4 where said output datum has the characteristic appearance of an asymmetric cryptographic key.

6. (Original) The wallet of claim 1 where said access code is a PIN, and said confidential datum includes a symmetric cryptographic key.

7. (Original) The wallet of claim 1 where said seed-access code relationship is a identity relationship, so that said derived seed equals said input access code.

8. (Original) The wallet of claim 1 where said seed-access code relationship represents said derived seed as a padded version of said input access code.

9. (Original) The wallet of claim 1 where said seed-access code relationship includes a version of said initial seed masked by user's access code.

10. (Original) The wallet of claim 9 where:

(i) said masked version of said initial seed includes an XOR of said initial seed with said user's access code; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes XORing said masked version of said initial seed with said derived seed.

11. (Original) The wallet of claim 10 further comprising program code for updating an user's old access code with a user's new access code by replacing said stored masked version of said initial seed with its value XORed with said user's old access code XORed with said user's new access code.

12. (Original) The wallet of claim 1 where:

(i) said seed-access code relationship includes a truncated version of said initial seed capable of being concatenated with said input access code to form said derived seed; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes concatenating said truncated version of said initial seed with said input access code.

13. (Original) The wallet of claim 1 where:

(i) said seed-access code relationship includes values of, and associations between, a plurality of possible values of said input access code and a corresponding plurality of possible values of said derived seed; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes looking up and outputting said possible value of said derived seed corresponding to said input access code.

14. (Original) The wallet of claim 13 where:

(1) said seed derivation module is merged with said data generation module;

(2) said output datum includes said derived seed.

15. (Original) The wallet of claim 5 where said confidential datum includes a private key of said user, and said output datum has the characteristic appearance of a private key.

16. (Original) The wallet of claim 5 where said user's public key corresponding to said user's private key is pseudo-public.

17. (Original) The wallet of claim 16 further comprising a digital certificate containing said pseudo-public key.

18. (Original) The wallet of claim 17 where said digital certificate includes an encrypted version of said user's pseudo-public key encrypted under a certifier's key which is not verifiable except by authorized verifiers.

19. (Original) The wallet of claim 1 configured to be remotely accessible to a roaming user across a network.

20. (Currently Amended) A computer-implemented method for securely storing and reproducing a confidential datum for said user, comprising:

(a) receiving an input access code;

(b) deriving a seed usable to generate at least a portion of said confidential datum by using said received input access code;

(c) obtaining a representation of a seed-access code relationship;

(d) digitally processing said derived seed

(i) in accordance with said seed-access code relationship,

(ii) by executing a predetermined data generation protocol that was previously used by a seed-based initialization of said confidential datum of said user,

(iii) thereby producing an output datum reproducing said at least a portion of said user's confidential datum if said input access code equals said user's access code; and

(e) said generation of said output datum occurring without dependence on any storage of any form of said at least a portion of said confidential datum~~.~~,

(f) wherein for at least one input access code not equaling said user's access code, producing an output datum that has the characteristic appearance of said at least a portion of said confidential datum, but said output datum does not reproduce at least a portion of said user's confidential datum.

21. (Canceled)

22. (Canceled)

23. (Original) The method of claim 20 where said access code is a PIN, and said confidential datum includes an asymmetric cryptographic key.

24. (Original) The method of claim 20 where said seed-access code relationship is a identity relationship, so that said derived seed equals said input access code.

25. (Original) The method of claim 20 where said seed-access code relationship represents said derived seed as a padded version of said input access code.

26. (Original) The method of claim 20 where said seed-access code relationship includes a version of said initial seed masked by user's access code.

27. (Original) The method of claim 26 where:

(i) said masked version of said initial seed includes an XOR of said initial seed with said user's access code; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes XORing said masked version of said initial seed with said derived seed.

28. (Original) The method of claim 20 where:

(i) said seed-access code relationship includes a truncated version of said initial seed capable of being concatenated with said input access code to form said derived seed; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes concatenating said truncated version of said initial seed with said input access code.

29. (Original) The method of claim 20 where:

(i) said seed-access code relationship includes values of, and associations between, a plurality of possible values of said input access code and a corresponding plurality of possible values of said derived seed; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes looking up and outputting said possible value of said derived seed corresponding to said input access code.

30. (Original) The method of claim 29 where:

(1) said deriving said seed and said executing said predetermined data generation protocol are merged into a common operation; and

(2) said output datum includes said derived seed.

31. (Canceled) A computer-readable medium having stored thereon a program executable on a computer to securely store and reproduce a confidential datum for said user, the program comprising computer logic instructions for:

(a) receiving an input access code;

(b) deriving a seed usable to generate at least a portion of said confidential datum by using said received input access code;

(c) obtaining a representation of a seed-access code relationship;

(d) digitally processing said derived seed

(i) in accordance with said seed-access code relationship,

(ii) by executing a predetermined data generation protocol that was previously used by a seed-based initialization of said at least a portion of said confidential datum of said user,

(iii) thereby producing an output datum reproducing said at least a portion of said user's confidential datum if said input access code equals said user's access code; and

(e) said generation of said output datum occurring without dependence on any storage of any form of said at least a portion of said confidential datum~~.~~,

(f) wherein for at least one input access code not equaling said user's access code, said output datum has the characteristic appearance of said at least a portion of said confidential datum, but said output datum does not reproduce at least a portion of said user's confidential datum.

32. (Canceled)

33. (Canceled)

34. (Original) The computer-readable medium of claim 31 where said access code is a PIN, said confidential datum includes an asymmetric cryptographic key.

35. (Original) The computer-readable medium of claim 31 where said seed-access code relationship is a identity relationship, so that said derived seed equals said input access code.

36. (Original) The computer-readable medium of claim 31 where said seed-access code relationship represents said derived seed as a padded version of said input access code.

37. (Original) The computer-readable medium of claim 31 where said seed-access code relationship includes a version of said initial seed masked by user's access code.

38. (Original) The computer-readable medium of claim 37 where:

(i) said masked version of said initial seed includes an XOR of said initial seed with said user's access code; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes XORing said masked version of said initial seed with said derived seed.

39. (Original) The computer-readable medium of claim 31 where:

(i) said seed-access code relationship includes a truncated version of said initial seed capable of being concatenated with said input access code to form said derived seed; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes concatenating said truncated version of said initial seed with said input access code.

40. (Original) The computer-readable medium of claim 31 where:

(i) said seed-access code relationship includes values of, and associations between, a plurality of possible values of said input access code and a corresponding plurality of possible values of said derived seed; and

(ii) said processing of said derived seed in accordance with said seed-access code relationship includes looking up and outputting said possible value of said derived seed corresponding to said input access code.

41. (Original) The computer-readable medium of claim 40 where:

(1) said deriving said seed and said executing said predetermined data generation protocol are merged into a common operation; and

(2) said output datum includes said derived seed.

42. (Currently Amended) A method for camouflaging a user's generation-camouflaged access-controlled datum under said user's access code, comprising:

(a) initializing a user's access-controlled datum by using a generation protocol in accordance with a generation indicia;

(b) storing in a memory in a digital wallet a predetermined relationship between said generation indicia and said user's access code;

(c) camouflaging at least a portion of said access-controlled datum

(i) such as to be reproducible by an authorized user thereof but non-reproducible by an unauthorized user thereof,

(ii) said camouflaging including storing said predetermined relationship between said generation indicia and said user's access code;

(iii) thereby allowing subsequent accessing of said at least a portion of said access-controlled datum via computer-based processing of an inputted access code, in accordance with said stored generation indicia-access code relationship;

(iv) without dependence on any storage of any form of said at least a portion of said access-controlled datum;

(v) wherein for at least one inputted access code not equaling said user's access code, generating an output datum that has the characteristic appearance of said at least a portion of said access-controlled datum, but said output datum does not reproduce at least a portion of said user's access-controlled datum; and

(d) ~~storing said camouflaged at least a portion of said access-controlled datum in a digital wallet; and~~

~~(e)~~ providing said digital wallet to said user.

43. (Original) A method for camouflaging a user's generation-camouflaged access-controlled datum under said user's access code, comprising:

(a) initializing a user's access-controlled datum by using a generation protocol in accordance with a generation indicia;

(b) generation-camouflaging at least a portion of said access-controlled datum such as to be reproducible by an authorized user thereof but non-reproducible by an unauthorized user thereof;

(c) storing said generation-camouflaged at least a portion of said access-controlled datum in a digital wallet; and

(d) providing said digital wallet to said user.